Программный комплекс Систэм Платформ

SePlatform.Tools 1.0
Service - LogViewer

Руководство пользователя

Редакция	Соответствует версии ПО
6. Предварительная	1.0.14

Содержание

1. Введение

Приложение Service - LogViewer предназначено для удобного просмотра журналов событий Windows с целью диагностики работоспособности системы.

Приложение Service - LogViewer входит в состав программного пакета SePlatform.Tools.

1.1. Системные требования

Операционная система	Microsoft Windows 7 SP1/Server 2008 R2 и выше
Разрядность ОС	x64 или x32
Процессор	Intel Celeron 1.6 ГГц и выше
Объем оперативной памяти	1 ГБ
Объем дисковой памяти	500 МБ
Сетевой адаптер	Ethernet 10/100/1000 Мбит/с
Программное обеспечение	› Microsoft Visual C++ 2015 x86 Redistributable Можно скачать по ссылке https://www.microsoft.com/ru-ru/download/details.aspx?id=48145

1.2. Установка и удаление

Для установки или удаления запустите установочный файл `*.msi`. В результате отобразится окно мастера установки. Для дальнейшей установки или удаления следуйте инструкциям мастера.

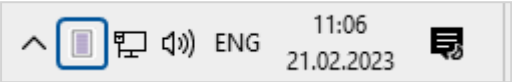
Установка приложения выполняется в папку: `C:\Program Files\SePlatform\SePlatform.Tools\EventLogViewer`.

2. Запуск

Варианты запуска:

- Стандартный
- С параметрами

После запуска на панели задач Windows появится иконка приложения.



Чтобы скрыть запущенное окно приложения, нажмите клавишу **«Esc»**. Чтобы отобразить запущенное, но скрытое окно приложения, используйте сочетание клавиш **«Alt»+«Space»** или кликните мышкой по иконке приложения на панели задач Windows.

2.1. Стандартный запуск

Для стандартного запуска приложения, воспользуйтесь командой `Пуск → SePlatform → Service - LogViewer`. Аналогичное действие можно выполнить, запустив исполняемый файл `EventLogViewer.exe`, расположенный в папке установки.

2.2. Запуск с параметрами

Использование параметров при запуске Service - LogViewer позволяет пользователю задавать предварительные установки конфигурационных данных, заменяющие настройки по умолчанию. Для запуска приложения с параметрами используется командная строка, вызываемая командой cmd в строке поиска, либо с помощью команды Пуск → Стандартные → Командная строка.

Параметры запуска

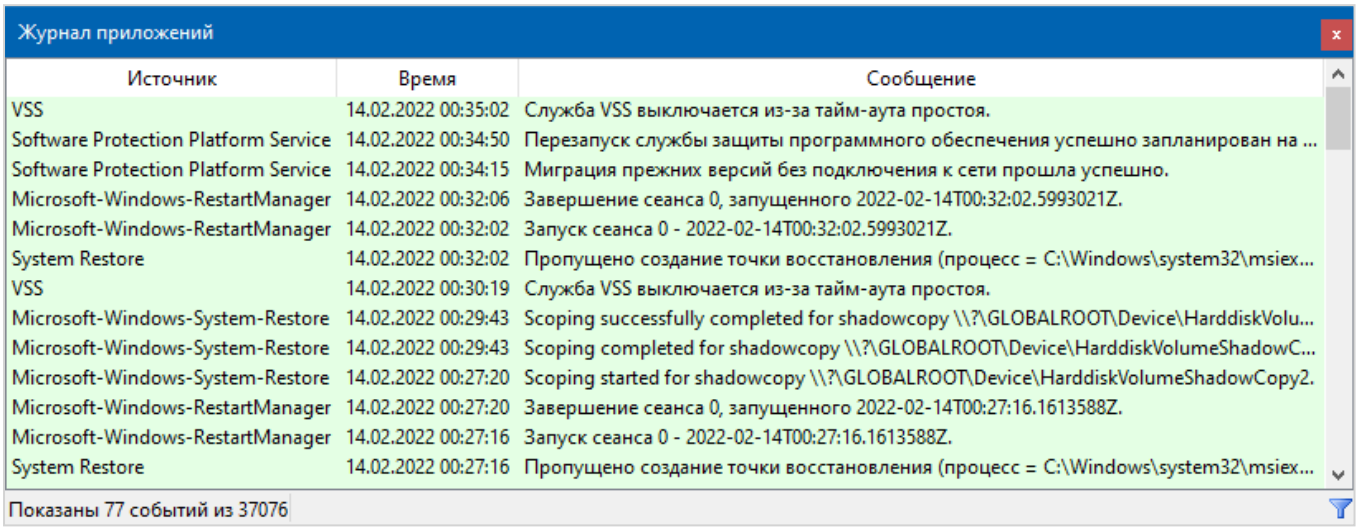
Параметр	Описание и пример
Log	Открывает указанный вид журнала или сохраненный файл журнала. Возможные значения: › **«Application»** - журнал приложений › **«System»** - системный журнал › **«Security»** - журнал безопасности › Полный путь до сохраненного файла Путь до сохраненного файла указывайте в кавычках. Разрешается указание пути без кавычек только в случае, если в пути не содержатся пробелы. Значения **«Application»**, **«System»**, **«Security»** не чувствительны к регистру.
	`C:\Program Files\SePlatform\SePlatform.Tools\EventLogViewer\EventLogViewer -log "C:\logfile1.evtx"`
	`C:\Program Files\SePlatform\SePlatform.Tools\EventLogViewer\EventLogViewer -log Application`
Windowpos, Windowsize	Размер и положение главного окна при запуске. Устанавливаемые параметры: › windowpos - расстояния от левой и верхней границ экрана до окна приложения. Оба значения указываются через запятую; › windowsize - ширина и высота окна приложения. Оба значения указываются через запятую
	`C:\Program Files\SePlatform\SePlatform.Tools\EventLogViewer\EventLogViewer -windowpos 0,0 -windowsize 950,550`
AlwaysOnTop	Окно Service - LogViewer запускается поверх окон других запущенных приложений.
	`C:\Program Files\SePlatform\SePlatform.Tools\EventLogViewer\EventLogViewer -AlwaysOnTop`

Параметр	Описание и пример
WindowsFixed	Для главного окна приложения и его дочерних окон (кроме системных окон ОС Windows[1]) заблокирована возможность менять положение или размер.
	`C:\Program Files\SePlatform\SePlatform.Tools\EventLogViewer\EventLogViewer -WindowsFixed`
FileSystemSafeMode	Управление режимом ограничения доступа к файловой системе. Блокирует возможность вызова окна справки, сохранения журнала в файл и загрузки журнала из файла.
	`C:\Program Files\SePlatform\SePlatform.Tools\EventLogViewer\EventLogViewer -FileSystemSafeMode`
Help	Вызов окна справки о программе. После вывода окна справки приложение Service - LogViewer не запускается.
	`C:\Program Files\SePlatform\SePlatform.Tools\EventLogViewer\EventLogViewer -help`

[1]Стандартные диалоговые окна сохранения/загрузки файлов, настройки печати и т.д.

3. Введение в пользовательский интерфейс

По умолчанию при запуске приложения открывается журнал приложений. События, которые произошли последними, располагаются в верхней части списка.



Типы отслеживаемых событий:

- информационные - события о работе SePlatform.Data Server или его модулей. События выделяются зеленым цветом;
- отладочные - события, которые детально отображают работу SePlatform.Data Server или его модулей. События выделяются белым цветом;
- предупреждения - события о логических ошибках работы SePlatform.Data Server или его модулей. События выделяются оранжевым цветом;
- ошибки - события о критичных ошибках, которые влияют на работоспособность SePlatform.Data Server или его модулей. События выделяются красным цветом.

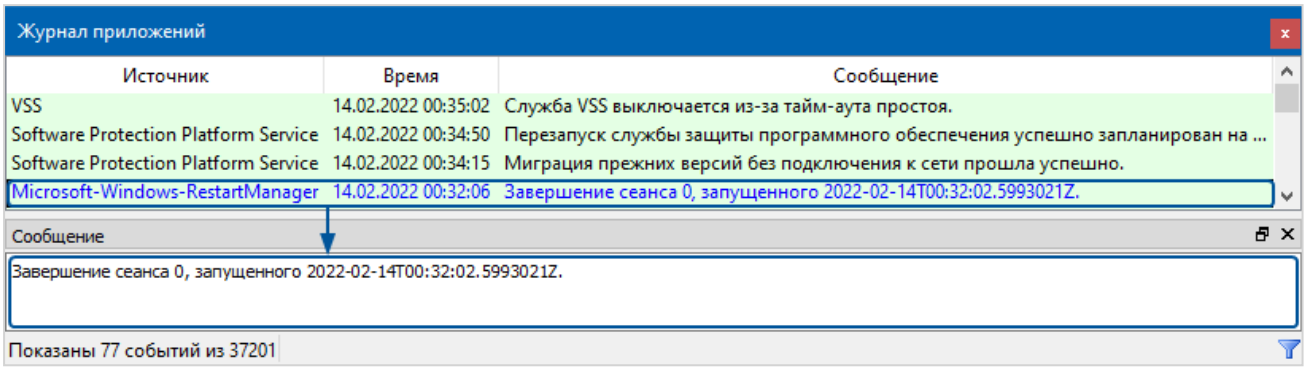
Запись о событии в журнале включает в себя:

- источник - программа или служба, которые зарегистрировали событие в журнале.
- время - дата и время возникновения данного события в журнале.

Для настройки даты и времени событий используйте команды меню **Вид** (стр. 10).

- сообщение - полное описание события.

Чтобы просмотреть полное описание события, дважды кликните по нужному сообщению. Полное сообщение отобразится на вкладке **Сообщение**.



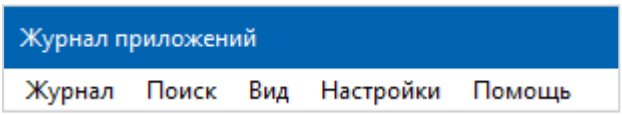
ПРИМЕЧАНИЕ

Вкладку **Сообщение** можно зафиксировать в верхней/нижней части окна приложения. Чтобы разместить вкладку **Сообщение** в верхней области окна, перетащите мышью ее к верхней части окна;

ПРИМЕЧАНИЕ

Вкладку **Сообщение** можно выделить в качестве отдельного окна приложения. Чтобы выделись ее отдельным окном, дважды щелкните мышью по заголовку вкладки. Процесс возвращения вкладки во внутрь главного окна аналогичен.

Чтобы отобразить/скрыть строку меню приложения, нажмите клавишу **«Alt»** или **«F10»**.



Чтобы скрыть запущенное окно приложения, нажмите клавишу **«Esc»**. Чтобы отобразить запущенное, но скрытое окно приложения, используйте сочетание клавиш **«Alt»+«Space»** или кликните мышкой по иконке на панели задач Windows.

Чтобы перейти к началу/концу сообщений журнала, нажмите клавиши **«Home»**/**«End»**.

Чтобы полностью очистить журнал событий, в контекстном меню выберите **Очистить журнал** или нажмите клавишу **«Space»**.

ОБРАТИТЕ ВНИМАНИЕ

Функция **Очистить журнал** доступна, только если приложение запущено от имени администратора (стр. 19).

ОБРАТИТЕ ВНИМАНИЕ

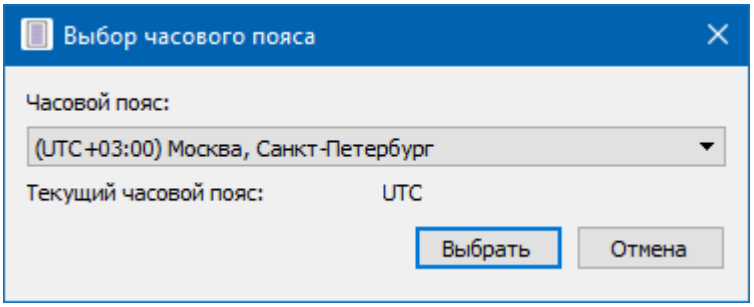
Использование функции **Очистить журнал** может привести к потери информации о работоспособности системы.

4. Настройка отображения журналов событий

Приложение Service - LogViewer позволяет настроить внешний вид журналов событий Windows:

- Задать часовой пояс для отображения даты и времени событий.
- Установить локальное время компьютера для отображения даты и времени.
- Установить окну приложения режим поверх всех окон.
- Скрыть/отобразить заголовки столбцов при просмотре событий.

Чтобы задать часовой пояс для событий, выберите команду **Вид** → **Задать часовой пояс...** и в окне **Выбор часового пояса** укажите необходимый часовой пояс.



Чтобы установить локальное время компьютера для событий, выберите команду **Вид** → **Локальное время**.

Чтобы окно приложения отображалось поверх всех окон, выберите команду **Вид** → **Поверх всех окон** или используйте параметр запуска AlwaysOnTop (стр. 5).

Чтобы скрыть/отобразить заголовки столбцов, нажмите сочетание клавиш **«Ctrl»+«H»** или выберите команду **Вид** → **Отображать заголовки столбцов**.

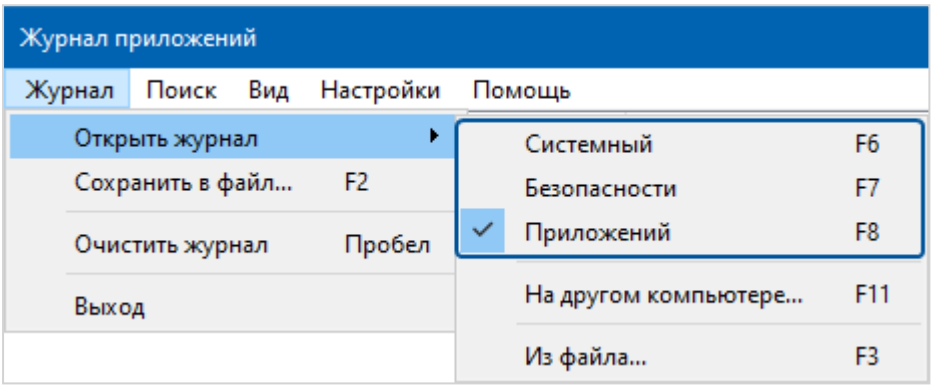
Чтобы скрыть/отобразить строку состояния, нажмите сочетание клавиш **«Ctrl»+«S»** или используйте команду **Вид** → **Отображать строку состояния**.

5. Просмотр журналов событий

Приложение Service - LogViewer позволяет просматривать события следующих журналов событий Windows:

- системный
- безопасности
- приложений

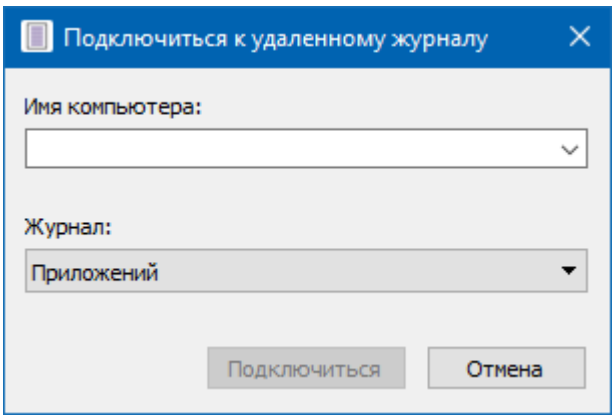
Чтобы переключаться между журналами событий, выберите нужный журнал в **Журнал** → **Открыть журнал** или используйте горячие клавиши.



ОБРАТИТЕ ВНИМАНИЕ

Функция **Открыть журнал** → **Безопасности** доступна, только если приложение запущено от имени администратора (стр. 19).

Чтобы просмотреть журнал событий на удаленном компьютере, выберите пункт **На другом компьютере...** и в окне **Подключиться к удаленному журналу** укажите имя удаленного компьютера и вид журнала событий.



Чтобы открыть сохраненный журнал событий нажмите клавишу **«F3»** или выберите команду **Журнал** → **Открыть журнал** → **Из файла...**.

ПРИМЕЧАНИЕ

При попытке удаленного подключения к своей машине происходит переключение на локальные журналы событий.

6. Создание журнала событий

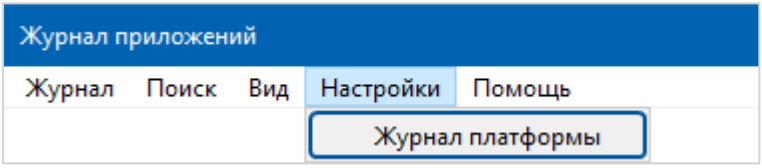
Приложение Service - LogViewer позволяет создать отдельный журнал для диагностики работы компонентов Систэм Платформ.

ОБРАТИТЕ ВНИМАНИЕ

Функция создания журнала событий доступна, только если приложение запущено от имени администратора (стр. 19).

Чтобы создать отдельный журнал событий:

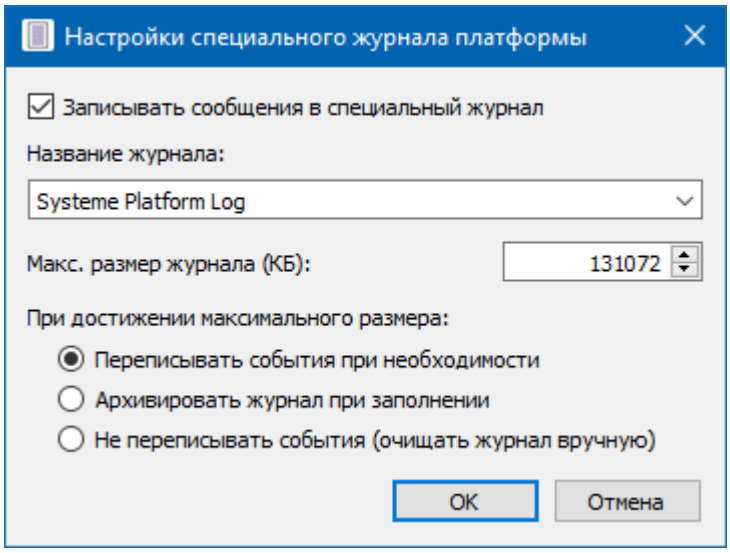
1. Отобразите строку меню приложения клавишей **«Alt»** или **«F10»**.
2. Выберите команду **Настройки** → **Журнал платформы**.



3. В появившемся окне **Настройки специального журнала платформы** установите флаг **Записывать сообщения в специальный журнал**.

ПРИМЕЧАНИЕ

Если флаг не установлен, запись событий компонентов Систэм Платформ будет происходить в **Журнал приложений**.



4. Задайте имя новому журналу.

Имя журнала можно ввести вручную или выбрать из списка всех существующих на машине журналов (кроме системного журнала и журнала безопасности).

Если введённое имя журнала отсутствует в списке доступных журналов, новый журнал событий будет создан. Созданный журнал отобразится в списке всех доступных журналов событий Windows.

ПРИМЕЧАНИЕ

В списке журналов, в контекстном меню, отображается последний открытый журнал событий компонентов Систэм Платформ.

Если требуется изменить журнал, в который будут записываться диагностические события компонентов Систэм Платформ, измените его в настройках приложения (**Настройки** → **Журнал платформы**).

Чтобы вернуть запись событий в **Журнал приложений**, выберите одно из следующих действий:

- Деактивируйте флаг **Записывать сообщения в специальный журнал**.
- Из списка доступных названий журнала выберите журнал **«Application»**.

7. Фильтрация событий

Для облегчения просмотра событий в журнале используйте фильтрацию событий.

Чтобы настроить фильтрацию:

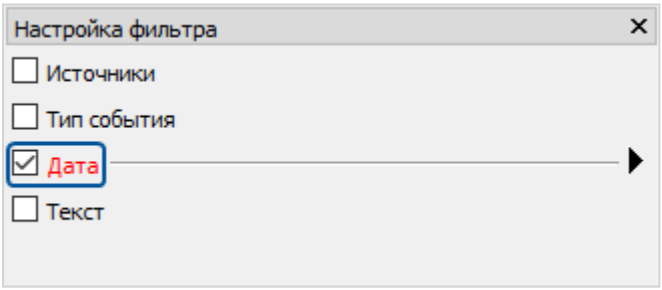
1. Откройте окно настройки фильтра любым способом:
   - В контекстном меню выберите **Фильтровать...**
   - нажмите клавишу **«F4»**
   - в меню выберите выберите **Поиск → Фильтровать...**
   - в статусной строке нажмите на иконку .
2. В окне **Настройка фильтра** поставьте флаг напротив необходимых фильтров:
   - **Источники**
   - **Тип события**
   - **Дата**
   - **Текст**

   При выборе фильтра, отобразятся его параметры фильтрации.
3. Для каждого выбранного фильтра укажите его параметры фильтрации.

   Фильтры применяются автоматически при включении/отключении фильтров и изменениях их параметров.

ОБРАТИТЕ ВНИМАНИЕ

Если фильтр включён, но его параметры не указаны или указаны неверно, фильтр не используется и его цвет меняется на красный.



ПРИМЕЧАНИЕ

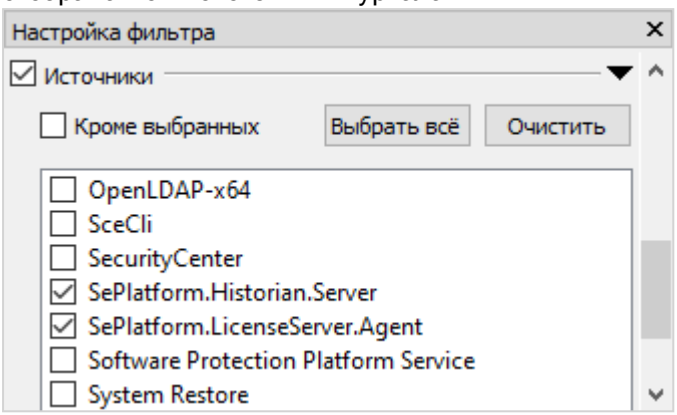
Если фильтрация событий включена, иконка фильтрации приобретает синий цвет: .

ПРИМЕЧАНИЕ

Окно **Настройка фильтра** закрепляемое: его можно закрепить в левой или правой части окна приложения.

7.1. По источникам

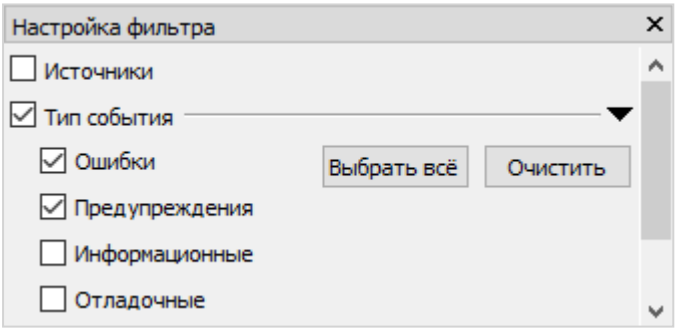
Фильтрация по источникам позволяет выбрать из списка программы или службы, события которых будут отображаться в системных журналах.



Чтобы выбрать все программы и службы из списка, нажмите **Выбрать всё**.
Чтобы очистить выбранный список программ или служб, нажмите **Очистить**.
Чтобы исключить из журнала событий определенные программы или службы, поставьте флаг напротив **Кроме выбранных** и отметьте эти программы или службы.

7.2. По типам событий

Фильтрация по типам позволяет выбрать типы событий, которые будут отображаться в системных журналах.

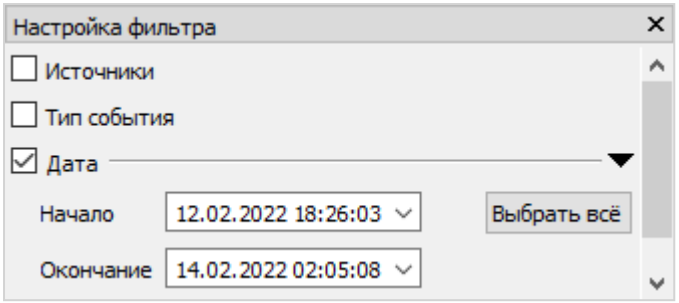


Чтобы выбрать все типы событий, нажмите **Выбрать всё**.

Чтобы сбросить фильтрацию по выбранным типам событий, нажмите **Очистить**.

7.3. По дате

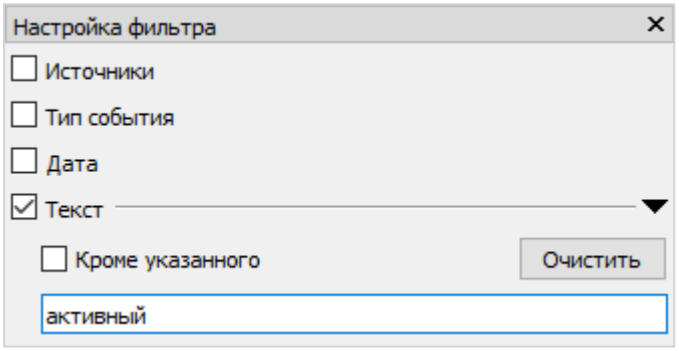
Фильтрация по дате позволяет выбрать дату и время регистрации событий в системных журналах и отобразить их.



Чтобы настроить фильтрацию по дате, выберите дату и время, с которых и по которые будут отображаться события в журнале.

7.4. По тексту

Фильтрация по тексту позволяет отобразить события в системных журналах, в сообщении которых присутствует текст, введенный пользователем.



Чтобы вывести события, в сообщения которых не входит текст, введенный пользователем, поставьте галочку напротив **Кроме указанного**.

Чтобы сбросить фильтрацию по тексту, нажмите **Очистить**.

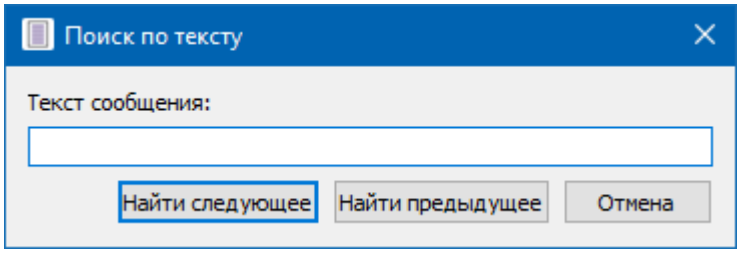
8. Поиск событий в журнале

8.1. По тексту сообщения

Позволяет искать события в списке событий системных журналов, в сообщениях которых присутствует текст, введенный пользователем.

Для поиска событий по тексту сообщения:

1. В контекстном меню выберите **Найти текст...** или нажмите сочетание клавиш **«Ctrl»+«F»**, или выберите команду **Поиск → Найти текст...**.
2. В окне **Поиск по тексту** введите текст сообщения.



3. Нажмите **Найти следующее**.

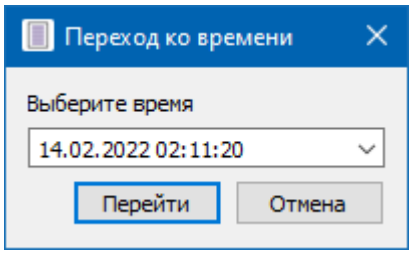
Чтобы перейти к предыдущему событию поиска, нажмите **Найти предыдущее**.

8.2. По времени

Позволяет искать события в списке событий системных журналов по времени и дате, которые ввел пользователь.

Для поиска событий по времени:

1. В контекстном меню выберите **Перейти ко времени...** или выберите команду **Поиск → Перейти ко времени...**.
2. В окне **Переход ко времени** выберите дату и время события.



3. Нажмите **Перейти**.

ПРИМЕЧАНИЕ

Если в списке событий не будет событий, удовлетворяющих запросу пользователя, системное приложение найдет события, которые приближены к запросу пользователя.

9. Сохранение журналов событий

Приложение Service - LogViewer позволяет сохранять события журналов в файлы с расширением `*.evtx`, `*.csv`, `*.txt` и `*.xml`.

ОБРАТИТЕ ВНИМАНИЕ

Сохранение журналов событий с удаленных компьютеров и журналов событий из файла невозможно в формате `*.evtx`.

Для сохранения журнала событий:

1. В контекстном меню выберите **Сохранить в файл...**, нажмите клавишу **«F2»**, или выберите команду **Журнал → Сохранить в файл...**.
2. В открывшемся окне выберите путь сохранения файла и расширение файла.

При открытии журнала событий из файла в заголовке окна приложения показывается путь к файлу.

10. Приложения

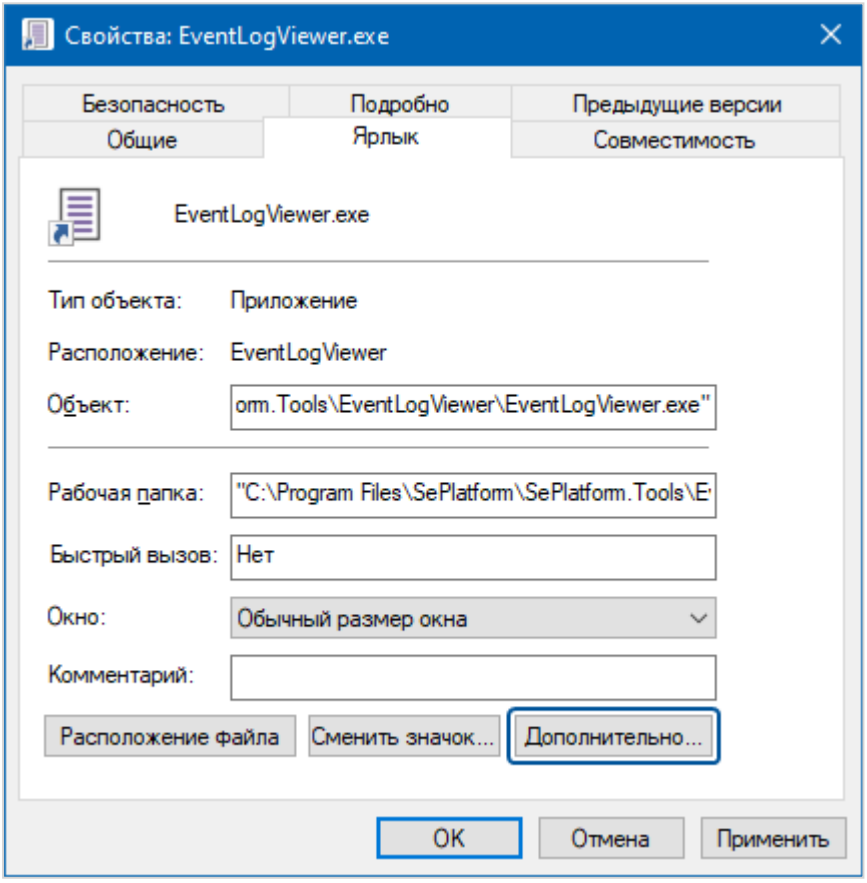
Приложение А: Настройка запуска приложения от имени администратора

В случае запуска приложения с правами администратора у пользователя появляется возможность просмотра журнала безопасности и очистки журнала.

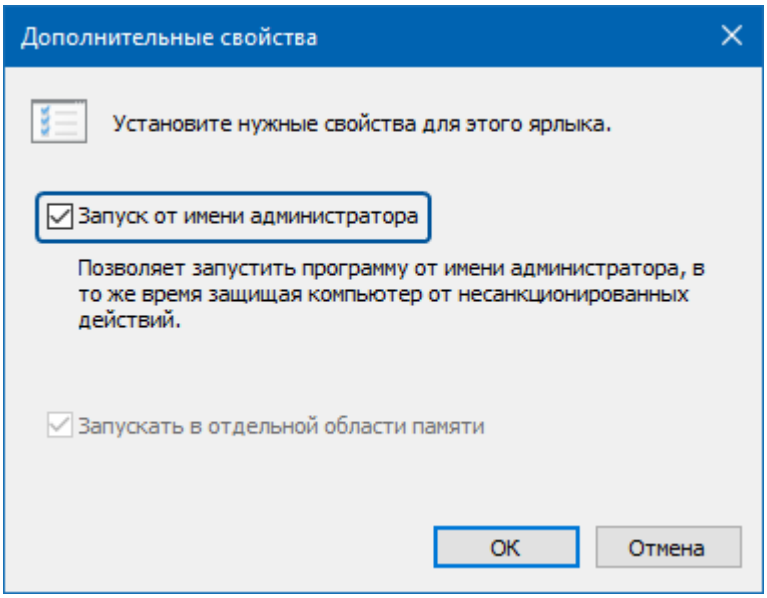
Чтобы пользователь без прав администратора смог запустить приложение Service - LogViewer от имени администратора, настройте ярлык приложения.

Функция запуска приложения с правами администратора настраивается в свойствах ярлыка приложения двумя способами - на вкладке **Ярлык** или на вкладке **Совместимость**.

- На вкладке **Ярлык**:
  1. Нажмите кнопку **Дополнительно...**.



2. В окне **Дополнительные свойства** поставьте флаг **Запуск от имени администратора**.



ПРИМЕЧАНИЕ

Если флаг **Запуск от имени администратора** не установлен, включите функцию запуска приложения с правами администратора на вкладке **Совместимость**.

› На вкладке **Совместимость**:

1. В области **Уровень прав** поставьте флаг **Выполнять эту программу от имени администратора**.